

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- - - - -x

UNITED STATES OF AMERICA

- v. -

VLADIMIR TSASTSIN,
ANDREY TAAME,
TIMUR GERASSIMENKO,
DMITRI JEGOROV,
VALERI ALEKSEJEV,
KONSTANTIN POLTEV, and
ANTON IVANOV,

Defendants.

- - - - -x

:
:
APPLICATION OF ASSISTANT
UNITED STATES ATTORNEY
JAMES PASTORE IN
SUPPORT OF EXTENSION OF
EX PARTE, POST-
INDICTMENT PROTECTIVE
ORDER PURSUANT TO
21 U.S.C. § 853(e)(1)(A)
AND (f), AND
18 U.S.C. § 1956(b)(4)
11 Cr. 878

I. **Preliminary Statement**

1. The Government respectfully submits this application seeking an extension of certain aspects of the *ex parte*, post-indictment protective order entered on or about November 3, 2011, by the Honorable William H. Pauley III in his capacity as the District Judge sitting in Part I (the " Original Order").

2. Among other things, the Original Order authorized the Government to take steps to ensure the availability of certain property for forfeiture, and to prevent further harm to millions of victims whose computers were infected with the malicious software that enabled the defendants' fraudulent schemes, as discussed in more detail below.

3. Most significantly for this application, the Original Order authorized the temporary replacement of certain Domain Name System ("DNS") computers used by the defendants to commit their fraud (referred to as "Rogue DNS Servers") with legitimate servers (the "Replacement DNS Servers") for a period of 120 days beginning on November 8, 2011, and ending on March 8, 2012.

4. The Replacement DNS Servers have enabled victims to continue to access websites even after the Rogue DNS Servers were deactivated. As set forth in a report submitted to the Court on or about January 23, 2012, since approximately November 8, 2011, the Replacement DNS Servers have handled queries from more than 16 million unique Internet Protocol ("IP") addresses, and continue to receive queries from more than 400,000 unique IP addresses a day.

5. For the reasons set forth below, the Government now seeks an order authorizing the continued operation of the Replacement DNS Servers for an additional approximately 120-day period. Specifically, instead of ceasing operation on March 8, 2012, the Government seeks authorization for the Replacement DNS Servers to continue to operate until July 9, 2012.

6. The Government respectfully submits that there is good cause to extend the Original Order previously entered by Judge Pauley.

II. **Background**

7. On November 1, 2011, a grand jury in the Southern District of New York returned a superseding indictment, S2 11 Cr. 878 (LAK) (the "Indictment"), charging VLADIMIR TSASTSIN, ANDREY TAAME, TIMUR GERASSIMENKO, DMITRI JEGOROV, VALERI ALEKSEJEV, KONSTANTIN POLTEV, and ANTON IVANOV, the defendants, with various crimes in connection with a massive and sophisticated Internet fraud scheme that infected at least four million computers with malicious software, or "malware." As detailed in the Indictment, the malware digitally hijacked victims' computers to facilitate the defendants' commission of Internet advertising fraud, thereby generating millions of dollars in illicit advertising "revenue" for the defendants. (Indictment ¶ 2). The Indictment identifies certain property that, in the event of conviction, will be subject to forfeiture (the "Forfeitable Property"). (Indictment ¶¶ 53-59).

8. As set forth in greater detail in the Indictment, the defendants and their co-conspirators operated and controlled companies that masqueraded as legitimate participants in the Internet advertising industry, entering into agreements with third parties under which the defendants' companies would be paid based upon the number of times that Internet users "clicked" on the links for certain advertisements, or based upon

the number of times that certain advertisements were displayed on certain websites. (Indictment ¶¶ 2, 17-19.)

9. The defendants and their co-conspirators defrauded the third parties paying them for their supposed advertising services by infecting millions of computers (the "infected computers") with malware that surreptitiously redirected those computers to the websites and advertisements. In this way, the defendants "earned" millions of dollars in advertising revenue even though the Web traffic they sent to the websites and advertisements consisted of Web users who had not intended to visit those websites or see those advertisements. (Id. ¶¶ 2-8.).

10. As set forth in more detail in the Indictment and in the affidavit of Special Agent Sean Zadig ("Zadig Decl.") of the National Aeronautics and Space Administration ("NASA") submitted in support of the Original Order, the defendants operated a network of computers to carry out their criminal scheme, including the Rogue DNS Servers.¹ Computers infected

¹ By way of background, a computer user can access a website on the Internet by either of two principal ways: by entering into the computer's web browser either the IP address, or the domain name, for that website. The IP address is a unique numerical address associated with a website (e.g., 123.45.6.78), akin to a home or business street address; whereas a domain name is a simple, easy-to-remember way for humans to identify computers on the Internet (such as "www.irs.gov"). When a computer seeks to access a website by its domain name, it uses a DNS server to first convert or "resolve" the domain name into

with the malicious software ("DNS Changer Malware") had their settings changed such that they relied on the defendants' Rogue DNS Servers to resolve DNS queries, and to thereby access websites on the Internet. (Indictment ¶¶ 20-33; Zadig Decl. ¶¶ 25-34).

11. From the investigation to date, we know that the infected computers include computers belonging to individuals worldwide, educational institutions, non-profit organizations; commercial businesses, and United States government agencies, such as NASA. (Indictment ¶ 5).

12. On or about November 8, 2011, all of the indicted defendants were arrested in Estonia, with the exception of ANDREY TAAME, who remains at large. The Indictment was unsealed on or about November 9, 2011, and, ultimately, the case was assigned to Your Honor.

13. When the aforementioned arrests occurred, law enforcement agents took steps to deactivate the defendants' computer network and related infrastructure, including their Rogue DNS Servers. The Government anticipated that, unless

the IP address for that website. The computer's internet service provider ("ISP") typically transmits the IP addresses for one or more legitimate DNS servers operated by the ISP, and that information is stored in the computer's operating system. (The DNS settings of a user's computer also can be changed without the user's permission by malware.) After the computer receives the IP address from a DNS server, it then uses that IP address to find the requested website and retrieve and display the relevant webpages.

certain remedial actions were taken, the practical effect of deactivation on victims whose computers were infected with the malware was that they would likely lose access to websites on the Internet, because the infected computers would be unable to resolve DNS queries after the Rogue DNS Servers were deactivated. (Zadig Decl. ¶¶ 72-74).

14. Accordingly, the Government sought a protective order to allow it to take necessary and appropriate steps to remediate and prevent the anticipated disruption of Internet service to millions of victims, and to ensure that the computers the defendants used to commit their crimes would be preserved for forfeiture.

15. As noted above, the Original Order obtained by the Government authorized, among other things, the temporary replacement of the defendant's Rogue DNS Servers with legitimate DNS servers. In addition, the proposed order appointed a third-party receiver - specifically, a non-profit entity called Internet Systems Consortium ("ISC") - to supervise the operation of the Replacement DNS Servers, so as to minimize to the greatest extent possible Government involvement (or the appearance of Government involvement) in Web communications.

16. Finally, the Original Order restrained the defendants and certain (a) Internet Service Providers ("ISPs"), (b) Regional Internet Registries ("RIRs") which administer IP

addresses, and (c) data centers, from taking steps that would thwart the Government's remediation efforts, or result in property being unavailable for forfeiture.²

17. The Government now respectfully seeks an order (a) authorizing the continued operation of the Replacement DNS Servers to July 9, 2012; and (b) extending the appointment of ISC as a third-party receiver to administer the Replacement DNS Servers until July 9, 2012.

III. **There Is Good Cause For An Extension**

18. The Government now seeks an extension of the Original Order for three reasons: First, several of the defendants' victims - specifically, network operators who have been informed of and/or detected infected computers on their networks - have contacted the Government and have indicated that they need additional time to remediate the harm caused by the

² The Government requested the assistance of Dutch authorities to give effect to the Original Order, because the RIR responsible for administering IP addresses in Europe (among other places) is headquartered in the Netherlands. That RIR - known as Réseaux IP Européens Network Coordination Centre ("RIPE") - initially complied with the Original Order. However, in or about January 2012, the Government was informed that RIPE had changed its position, and now refuses to comply with the Original Order. Accordingly, to the extent RIPE now transfers any of the IP addresses previously associated with the defendants, that could facilitate criminal activity, especially because at least one defendant remains at large. Any such transfer also may disrupt remediation efforts, and result in victims losing Internet access. To date, however, RIPE's refusal to comply with the Original Order has not had any adverse effect on the remediation efforts.

malicious software. Second, although the Federal Bureau of Investigation ("FBI") already has provided direct notice to at least 10,000 network operators, it has identified and is in the process of notifying approximately 15,200 network operators outside of the United States; additional time is needed to complete this victim notification process. Third, based on information provided by ISC, although the number of daily, unique visitors to the Replacement DNS Servers has generally declined since November 8, 2011, it appears that at least several hundred thousand computers continue to rely on the Replacement DNS Servers to resolve DNS queries.

19. Both the United States Attorney's Office for the Southern District of New York and the FBI have been contacted by victims who have expressed concern about the impending deactivation of the Replacement DNS Servers. For example, in a communication dated January 27, 2012, a representative of one Internet Service Provider ("ISP-1") estimated that approximately 50,000 of its customers are infected with the malware the defendants utilized to perpetrate their frauds. According to ISP-1, absent continued operation of the Replacement DNS Servers, its customers are at risk of being unable to access the Internet.

20. Other victims have communicated similar concerns in telephone conversations with the FBI. That is, several

victim ISPs have indicated that additional time is necessary to enable them to remove the malicious software from infected computers on their networks.

21. The Government also seeks an extension of the Original Order in order to provide additional time for victim notifications from the FBI to reach several thousand network operators located outside the United States. As noted above, the FBI has notified more than 10,000 victim entities in the United States, such as various ISPs. These entities, in turn, administer networks that could have hundreds, thousands, or even tens of thousands of infected computers.

22. In addition to network operators in the United States, the FBI has begun distributing more than 15,000 notices to victim entities located outside of the United States. In order to reach these victim entities, however, the notices are being distributed through 61 Legal Attache offices maintained by the FBI around the world. In order to allow these notices to reach the victim entities, and to provide adequate time for those entities to take actions based on these notices (for example, by notifying individual subscribers that their computers are infected, and then instructing them how to remove the malware), the Government respectfully submits that an extension of the Original Order is appropriate.

23. Finally, the information provided by ISC to the Court on or about January 23, 2012, indicates that several hundred thousand computers continue to rely on the Replacement DNS Servers to resolve DNS queries.

24. The report provided by ISC indicated that, generally speaking, the number of unique IP addresses that queried the Replacement DNS Servers in a 24-hour period declined between November 8, 2011 and January 8, 2012. However, the report also indicated that at least 430,000 unique IP addresses queried the Replacement DNS Servers each day during the two-week period preceding January 8, 2012. In other words, several hundred thousand computers continue to rely on the Replacement DNS Servers to access websites. Extending the operation of the Replacement DNS Servers will provide additional time for victims to remove the malware from their computers, thereby enabling them to reach websites without relying on the Replacement DNS Servers.

25. In light of these reasons, the Government respectfully submits that an extension of the operation of the Replacement DNS Servers, and ISC's appointment as a third-party receiver, is appropriate, and therefore respectfully requests that the Court enter the enclosed, proposed order.

Dated: New York, New York
February 17, 2012

/S/
JAMES J. PASTORE, JR.
Assistant United States Attorney
Southern District of New York